

Published and Copyright (c) 1999 - 2014
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

<http://people.delphiforums.com/dpj/a-one.htm>
Now available:
<http://www.atarinews.org>

Visit the Atari Advantage Forum on Delphi!
<http://forums.delphiforums.com/atari/>

=~::~~::~=

~ Google Trends Updated! ~ New Google Glass Offer! ~ CAPTCHAs Are Cracked!

```

    -* Heartbleed Fix Slows Browsers *-
    -* White House Updates Online Privacy! *-
    -* The New Longest Arcade Game Run in History *-

```

$$= \sim = \sim = \sim =$$

```
->From the Editor's Keyboard           "Saying it like it is!"
   " " " " " " " " " " " " " " " "
```

The Heartbleed problem seems to be dominating the online community these days, with those potential "targets" doing what they can to repair some holes in their systems. Surprisingly, this took awhile to become a public notice; it appears that Heartbleed has been around for some time. Ever vigilant has taken a security catnap.

Until next time...

== ~ == ~ == ~ ==

```
->In This Week's Gaming Section - Sony Sells More Than 7 Million PS4s!
    " " " " " " " " " " " " " " XBOX One Sales Top 5 Million!
                                     The History Of Atari!
                                     And much more!
```

$$= \sim = \sim = \sim =$$

->A-ONE's Game Console Industry News - The Latest Gaming News!
 ~~~~~

## Sony Sells More Than 7 Million Playstation 4 Consoles

Sony Corp sold more than 7 million PlayStation 4 units as of April 6 and is struggling to keep pace with demand for the video game console, the company said on Wednesday.

"Although we are still facing difficulties keeping up with the strong demand worldwide, we remain steadfast in our commitment to meet the needs of our customers," Andrew House, president and group chief executive officer of Sony Computer Entertainment, said in a statement.

In February, the Japanese company had said it sped past its full-year

target of 5 million units by the end of March this year. It had sold 6 million PlayStation 4 units as of March 2.

PlayStation 4 software sales - retail and digital - touched 20.5 million copies worldwide as of April 13, the company said in its statement.

The console went on sale on Nov. 29 in the United States, Western Europe and Latin America, around the same time that rival Microsoft Corp's Xbox One was released. That console topped 3 million units at the end of last year.

#### Xbox One Sales Top 5 Million

Microsoft said Thursday it has sold more than 5 million Xbox One consoles since they were launched in November.

The news came a day after video game competitor Sony said it had sold more than 7 million PlayStation 4 consoles since mid-November.

Sony's numbers refer to sales to consumers, while Microsoft's involve sales to retailers.

Sales of Xbox One were 60 percent higher than those of Microsoft's earlier iteration Xbox 360 during the same length of time after it hit the market, Yusuf Mehdi, vice president of marketing, strategy and business, wrote on the Microsoft blog in announcing the figures.

Furthermore, the new game Titanfall, which Microsoft was counting on to boost sales of the new Xbox, was the world's hottest-selling game in March, said Mehdi, quoting figures released Thursday by analysts NPD Group.

Titanfall, which came out in March, involves a futuristic galaxy torn by fighting between elite fighter pilots and huge, heavily armed titans.

#### 'Amazing Spider-Man 2' Might Not Make It To Xbox One

Activision has pulled the Xbox One box art from the website for its upcoming licensed game The Amazing Spider-Man 2.

For the time being at least, the game will make it to just about every other platform except Xbox One including the 360 and Wii U.

We are working with Microsoft in an effort to release The Amazing Spider-Man 2 video game on Xbox One, Activision said in a statement to the press. Currently, the game will be available on PlayStation 4, PlayStation 3, Xbox 360, Nintendo Wii U, Nintendo 3DS and the PC on April 29, 2014 as previously announced.

Beyond this, there are no details and no reasons given. We're left with only speculation and curiosity.

The removal of the box art was first spotted by a NeoGAF user. According to that post, a German retailer has sent out an email to customers saying

that the Xbox One version has been cancelled.

Whether it s a cancellation or a delayed release remains to be seen, but this is obviously going to raise some eyebrows without further explanation. Granted, a licensed IP like this isn t as big of a deal as something like Watch Dogs or Call of Duty not making it to a major platform, but it is odd.

Meanwhile, retailers will need to begin updating their websites accordingly. For instance, as of this writing I can still order the Xbox One version of the game on Amazon where an April 29th release date is still in the listing.

### Bungie Fires Halo Composer Martin O'Donnell

Halo series and Destiny composer Marty O'Donnell was fired by Bungie's board of directors last week, the composer revealed via his personal Twitter account.

O'Donnell composed music for Oni, as well as the Myth and Halo series. He joined Bungie in 2000 as audio director after working on Myth 2, Oni and Halo: Combat Evolved's scores on a contract basis with his company TotalAudio. During his time at Bungie, O'Donnell directed voice talent and sound design for the Halo trilogy, Halo: Reach and Halo 3: ODST. He often collaborated with TotalAudio partner and now in-house audio design lead at Bungie, Mike Salvatori.

O'Donnell, Salvatori and Paul McCartney recently worked together to create the soundtrack for Bungie's new shooter, Destiny. O'Donnell said McCartney was drawn to the project by an interest in interactive music. The three also produced a symphonic and choral prequel suite for Destiny called Music of the Spheres, which premiered during game music concert performance Video Games Live last July.

The early draft of the score, O'Donnell explained, was largely written without any idea of what the game looked or played like. When he was finished, he jokingly said, "I dumped 50 minutes of music on [the development team and said 'Deal with that. Make a game as good as that.'"

He said his goal as audio director for Bungie, working on Destiny, was that every sound in the game would be created from scratch.

Titled "There are those who said this day would never come...", Bungie posted the following statement regarding O'Donnell's termination on its official website:

"For more than a decade, Marty O'Donnell filled our worlds with unforgettable sounds and soundtracks, and left an indelible mark on our fans. Today, as friends, we say goodbye. We know that wherever his journey takes him, he will always have a bright and hopeful future.

=~==~==

Under Warner it committed suicide. It wasn't homicide, it was self-inflicted stupidity, Bushnell said to Tech Radar last year. What you had was a bunch of record guys thinking they knew what the game business was about - I could catalogue the screw ups they made. I would have liked to have taken Atari to another level. If I could go back in time I would not sell to Warner.

Warner's reluctance to take risks is well exemplified by the the Cosmos, a handheld console that was going to use holography (the idea was to create a cartridge based game system at half the cost of the VCS, capable of producing 3D-ish images using hologram technology). Pong creator Al Alcorn and two other Atari engineers (Harry Jenkins and Roger Hector) started work on it in 1978, at which point Alcorn was bored of being an executive and wanted to get back into making things again, but despite years of development, pre-release adverts and more than 8,000 pre-orders from retailers, Warner refused to release it without a firm business plan that the engineers could not produce. The Cosmos was finished, but never released.

The company was big, and management was sluggish - a world away from the adaptive, nimble Atari that first established and then dominated the video arcade with its varied and risky coin-op machines. When we were young at Atari, every year we risked the whole company on new products, Al Alcorn said to IGN back in 2008. If the VCS had failed, or Home Pong had burned up, we'd have killed the company. And now Atari is making billions of dollars a year in revenue and if [something] had failed it wouldn't have been a pimple on the butt of the thing, yet the fear of failure and the ego of these guys they weren't Silicon Valley, they weren't start-up guys, they were not risk takers, so nothing came out.

Warner sold the home computing portion of the Atari business in July 1984 to Jack Tramiel, the erstwhile founder of Commodore, who renamed it Atari Corporation. It held onto the arcade division, now known as Atari Games, for a bit longer. But ultimately Warner would also unload the arcade business, selling it to Namco in 1985. One year later, a group of employees would buy Atari Games independence from Namco, and the group would go on to create late-era arcade classics like Paperboy and San Francisco Rush under various corporate banners, even returning to Warner at one point.

It was the the big Atari split - the point at which Atari's history become convoluted and kind of sad. Atari's golden age was over, almost all of the people who had first made it a success were gone, and the story from this point on would be one of the increasing dilution of the brand that was the most powerful name in video games for over a decade.

In the mid to late eighties, there were so many different home computers that games would come out in squillions of different versions. I'm looking at a review for a game called Terramex, in a copy of The Games Machine magazine from February 1988, and it's reviewed on the Spectrum 48, Spectrum 128, Commodore 64/128, Atari ST, Amstrad CPC and the MSX. Then there was the Amiga, too. And the PC, which was a different thing to all of them. This is totally baffling to a child of the console generation. It's bad enough with two or three of them to fight over. At least they didn't have Internet comments back then.

Atari's 8-bit computers, the 400 and the 800 and its successors, made a decent impact in home computing in the early 80s. But by 1985, there were plenty of other companies in on the games market that Atari had once all-but owned. Its failure to keep coming up with new products under Warner left its new owner Jack Tramiel playing catch-up.

Interestingly, some of those competitors were made by people who had once been part of Atari, or worked closely with it. Jay Milner, who had designed the chips for Atari's VCS and 8-bit computers, went on to form Amiga. Then there were Apple computers - you know, by that guy who helped create Breakout, Steve Jobs.

Atari Corp's next machine would be the Atari 520ST: a 16-bit computer that ran games off both floppy disk and cartridge, and would stick around for years. The Atari ST range was a lot of 80s kids' first computer, and even though the Amiga proved to be the better machine, it was a good deal cheaper - actually it was the cheapest 16-bit computer around. The ST was an idiosyncratic machine. Its MIDI port made it a favourite with musicians, and it was especially popular in Europe, where another line called the Atari PC also made an impact. The ST had a fairly impressive lifespan, too - the final ST model was called the Mega STE, released in 1990.

By 1990, though, change was sweeping through the games industry. Consoles were starting to gain traction once more as the games machines of choice. This happened earlier in the US, where the NES hit in 1985 and Sega's Master System in 1986. Those consoles dominated in America by '87, and though they didn't make the same impact in the UK and Europe, the 16-bit consoles of the early '90s would. In the home computer market, meanwhile, Microsoft's operating system ecosystem was becoming totally dominant.

In 1993, after releasing one last 32-bit computer called the Falcon the previous year, Atari Corporation shut down its home computer manufacturing business in order to concentrate on making its own console. This would prove the company's final undoing as a hardware manufacturer.

First, though, there was a brief and even more ill-fated diversion into portable consoles. The Atari Lynx wasn't actually developed internally by Atari; it was conceived by a company called Epyx, and sold to Atari in January 1989. It came out later that same year. Released the same year as the Game Boy, it was a technically far superior handheld, with full colour and games that boasted arcade quality - but it was far more expensive than the Game Boy, with only a 4-5 hours battery life, and Nintendo's handheld comprehensively won the early fight for market share thanks to Tetris. Once Sega's Game Gear came out in 1991 with Sega's much-better software lineup, it wasn't even the only color handheld around anymore. The Lynx died a quick death.

But it was ultimately the Atari Jaguar that drove the company into the ground. It was the first 64-bit console, released in 1993. The red-and-black machine looked kind of like something from Knight Rider's innards. It was impressively powerful for its time, but its terrible controller and lack of software support prevented the Jaguar from breaking through against the incredibly popular Super Nintendo & Sega Genesis. Only 67 Jaguar games were ever released.

The Jaguar was not without its hits - Tempest 2000 and Alien vs Predator are remembered fondly - but it wasn't enough. The Jaguar didn't last long, and Atari had nothing left to sell. In 1996, Tamriel admitted defeat, and the company disappeared into corporate purgatory.

That was the second time that Atari properly died, if the first time was when Warner sold it off in bits. Two years later Atari was resurrected when Hasbro Interactive, the video game division of the toy giant, bought JTS for a paltry \$5 million, primarily to acquire the rights to the Atari name. Hasbro then sold its video game subsidiary to French software company Infogrames in 2000. This is when many younger gamers started seeing the Atari brand and that distinctive logo return to prominence.

You see, Infogrames was an aggressively acquisitive company throughout the late 90s and early 00s, buying up several big name publishers and brands

in an attempt to rival EA. Once it had the Atari name, Infogrames decided to give itself global recognition, and rebranded its American and European publishing and distribution businesses to Atari in 2003. That's the Atari that we saw on the boxes of games like 2003's *Driver 3*, 2009's *Ghostbusters: The Video Game* and 2008's *Alone in the Dark*. It was a very complex company at that time - part distributor, part publisher, and one of many floundering companies under Infogrames' banner.

As for Atari's original games - *Pong*, *Centipede*, *Tempest*, the arcade-era classics - those stuck around, and were re-released in various compilations and on mobile throughout the '00s. But Atari was neither a force in games hardware nor games development any more. Atari's final death happened in January 2013, when it filed for bankruptcy yet again. As of yet, nobody's stepped up to buy the name.

Nor was the Atari that died in 1996. Looking back on its history, it seems like Atari wrote its own death warrant when it sold to Warner; it may have achieved its greatest monetary success under that ownership, but the creativity and risk-taking that established it were nowhere to be seen. You can't help but wonder how things might have been if that hadn't happened. Maybe Atari would be up against Sony, Microsoft and Nintendo today.

Its founder Nolan Bushnell thinks so. Absolutely Atari could be competing with Xbox and PlayStation today, he told TechRadar last year. I would have liked to have taken Atari to another level. If I could go back in time I would not sell to Warner. Take the company public, raise money that way - I think I should have just taken a vacation.

Atari may not have invented video games, but it invented the business of video games. It shaped the idea of what early games were: easy to learn, hard to master, and most importantly, accessible to everyone.

### The New Longest Arcade Game Run In History - Over 85 Hours

On the morning of Wednesday, April 9, Ohio arcade champion John Salter slipped a quarter into his *Armor Attack* arcade cabinet. By the time he finished playing late Saturday night, he'd broken two major video game records.

The last two guys to try and beat the *Q\*Bert* world record had to pull out due to fatigue, because they'd need to have played the game for over

In an event streamed live on the website of "Video Game Media Personality" Patrick Scott Patterson, Salter spent 85 hours 16 minutes playing *Armor Attack*, a 1980 vector-based shooter from Cinematronics. In doing so he has claimed the world record for longest arcade game run on a single credit. The previous record, 84 hours and 48 minutes, was set by *Q\*Bert* champion George Leutz last year.

Salter survived the gaming marathon by taking power naps, letting the game claim a fraction of his pool of extra lives while he did so. 1

While the longevity record was fresh, Salter also scored 2,211,990 points, breaking the 2,009,000 point record set in 1982.



=~==~==

A-ONE's Headline News  
The Latest in Computer Technology News  
Compiled by: Dana P. Jacobson

The White House Has Updated Its Online Privacy Policy

A new Obama administration privacy policy released Friday explains how the government will gather the user data of online visitors to WhiteHouse.gov, mobile apps and social media sites, and it clarifies that online comments, whether tirades or tributes, are in the open domain.

Information you choose to share with the White House (directly and via third party sites) may be treated as public information, the new policy says.

The Obama administration also promises not to sell the data of online visitors. But it cannot make the same assurances for people who go to third-party White House sites on Facebook, Twitter, or Google Plus.

There will be no significant changes in actual practices under the new policy. But legal jargon and bureaucratic language have been stripped out, making it easier for readers to now understand that the White House stores the date, time, and duration of online visits; the originating Internet Protocol address; how much data visitors transmit from WhiteHouse.gov to their computers; and more. The administration also tracks whether emails from the White House are opened, forwarded, or printed.

The updates were needed because Our old privacy policy was just that old, blogged Obama's digital director Nathaniel Lubin.

After coming to office in a campaign lauded for its online savvy, President Obama's White House has quickly adapted to online engagement since taking office in 2008, embracing using the Internet in all its manifestations. The first administration with an Office of Digital Strategy, Obama's online strategy now includes a We the People petitions platform, live online chats, and more than a dozen social media sites, including Google+, LinkedIn, Pinterest, Instagram, Vine, Myspace, and seven Facebook pages, including La Casa Blanca and Education to Innovate.

Visitors who link to those social media sites are advised: Your activity on those sites is governed by the third-party website's security and privacy policies, which frequently allow those companies to sell visitors' data. In addition, the White House archives Twitter, Facebook, and Google+ content to comply with the Presidential Records Act.

The policy says Obama will keep some information automatically generated email data, Mobile App use data, and some cookie data until the end of the current administration. The White House is also explicit about what it doesn't do, including collecting geolocation information from mobile-app visitors or sharing information for commercial purposes.

The policy is being released at a time when the administration is facing unprecedented criticism over disclosures from former intelligence contractor Edward Snowden that expose sweeping U.S. government surveillance programs. The policy aims to address at least some of those concerns.

White House spokesman Matt Leirich said they also do not give third parties, including the political organization Obama for America or the U.S. National Security Agency, access to their email database or other systems.

Within the White House, we restrict access to personally identifiable information to employees, contractors, and vendors subject to non-disclosure requirements who require access to this information in order to perform their official duties and exercise controls to limit what data they can view based on the specific needs of their position, the policy says.

For example, if someone gives the White House a telephone number or email address, staffers might respond to the message or petition, providing information or even services if appropriate. They might also take messages, comments, Twitter replies, and Facebook comments to use for public advocacy, like promoting Obama's health-care overhaul.

If a visitor asks the White House a question that is really about homeland security, that person's information may be shared with that agency. And if someone is trying to report a federal crime, or threatening someone, that person's information may be passed on to law enforcement.

Leirich said that when people share comments or sign online petitions through the We the People platform, it's with the understanding that it is public information.

Reviews from privacy experts who have been watching the privacy-policy revisions closely were mixed.

The biggest problem, said Jeramie Scott, national security counsel for the Electronic Privacy Information Center in Washington, D.C., is not what happens when visitors are on WhiteHouse.gov, but when they click onto the White House's third-party social media sites that don't abide by Obama's own privacy rules and may sell personal data they glean from visitors.

Interacting with the White House and its different sites is inherently political, and that type of thing shouldn't be used for commercial gain, Scott said.

Mark Jaycox, a legislative analyst at the Electronic Frontier Foundation in San Francisco, said the new policy underscores the administration's ongoing interest in collecting data. You see it across the board. You saw it in the campaign. You see it in the White House petitions. This is just one more step toward amassing more information, he said.

Jaycox said the new policy is not explicit enough about what the White House does with information it gathers. The onerous thing is we don't know what they're doing on the back end with all of this data, he said.

But several privacy experts praised the new policy as more explicit and understandable.

It's a nice gesture by the White House, said Federation of American

Scientists secrecy expert Steven Aftergood in Washington. I think the move reflects a heightened public awareness of privacy concerns, which is commendable.

Consumer Watchdog Privacy Project director John Simpson said that in terms of pure disclosure, this seems to be one of the better policies, a model perhaps for others.

### It's Real: Hackers Are Using Heartbleed To Attack Servers

When the Heartbleed vulnerability was made public last week, it seemed terrifying. Afflicting thousands of servers across the Internet, the bug had the potential to expose a wide variety of private data, including credit card numbers, passwords, and even a server's private encryption keys.

But one question that came up a lot was whether anyone had actually used Heartbleed to attack real computer systems. For the first few days, no one could point to real-world examples of Heartbleed attacks.

But now that uncertainty has been put to rest, as the security firm Mandiant reports that it has observed a Heartbleed attack occurring "in the wild." The attack targeted a Virtual Private Network service at an unnamed organization, gaining access to its internal corporate network and it shows that hackers are finding the parts of the internet are least likely to have been updated to protect against Heartbleed.

The attack worked like this. When a user logs into a VPN service, it issues a "session token," a temporary credential that is supposed to prove that a user has already been authenticated. By stealing the authentication token from the server's memory, the attacker can impersonate the legitimate user and hijack her connection to the server, gaining access to the organization's internal network.

In the immediate aftermath of Heartbleed's discovery the vulnerability of big organizations like Google and Tumblr got most of the press. Those firms quickly updated their software and hardened their defenses.

The problem is that OpenSSL is used by a lot of smaller companies in a wide variety of special-purpose networking appliances. The software on these network appliances may not be as easy to upgrade as a general-purpose web server. And organizations might not even realize that their devices are running OpenSSL in the first place, much less know how to fix it.

That means we should expect to see organizations being hit with Heartbleed attacks for a long time to come. It'll be a recurring reminder that we don't invest nearly enough to secure our IT infrastructure.

### Here's How The Heartbleed Bug Scurried Into The Hearts and Minds of Millions

On April 7, 2014, the world learned of what's possibly the most severe security bug in the history of the Internet. It's called Heartbleed.

Discovered simultaneously by Neel Mehta, a security researcher at Google, and Finnish security firm Codenomicon, the bug compromises a security protocol commonly used by devices and websites worldwide. Heartbleed makes it possible for a hacker to scrape data from memory including passwords, bank account numbers, and anything else lingering inside.

The severity of the bug left many wondering how it could happen. OpenSSL, the security protocol in which bug was found, is used all over the world. It's used not just in servers, but also routers and even some Android smartphones. You might think that some responsible party has a team of security researchers checking and double-checking the code but, in truth, OpenSSL is managed by a small group consisting mostly of volunteers. Opening to OpenSSL

OpenSSL boasts its open-source origin in its name. Founded in 1998, the project was created to provide a set of free encryption tools for Internet servers. This was an important goal; encryption is critical and common. A free standard was needed to make sure it would be adopted as quickly as possible. The project was wildly successful, and quickly became one of the Internet's most important security tools.

Yet, success did not result in expansion or profits. OpenSSL generates income only through support contracts, which provides access to troubleshooting and consulting from the organization itself.

A total of just 11 people, most of them volunteers, are responsible for a critical encryption standard.

These contracts provide a minor stream of revenue, but the project is far from being overflowing with cash. The OpenSSL Software Foundation has never earned more than one million dollars in gross annual revenue. Donations have been anemic as well; the organization usually receives about \$2,000 each year.

This results in a predictably tiny staff. The core team is made up of only four individuals, and the development team adds seven more names to the list. That's a total of just 11 people, most of them volunteers, responsible for a critical encryption standard. Only one of them, Dr. Stephen Hanson, focuses on OpenSSL entirely. Everyone else has another full-time job.

Steve Marquess, who manages the organization's money, said it best. The mystery is not that a few overworked volunteers missed the bug; the mystery is why it hasn't happened more often. Mistakes were made

That's what the entire crisis boils down to—a mistake. The error was introduced by Robin Seggelmann, a German volunteer working on an OpenSSL extension called Heartbeat. He submitted the code on New Year's Eve, 2011, and it subsequently slipped through the review process. Heartbleed has existed, unknown to the public, for over two years.

Other members of the project double-check submitted code during the review, but mistakes happen, so it's hardly a surprise that a bug eventually slipped through. Even multi-billion dollar companies like Microsoft and Cisco are hit by their fair share of embarrassing exploits.

The problem stems from allocating memory according to a value that can be defined by a request. If the user provides a valid input, the function works as intended. However, if an invalid request is made, the code dumps

part of what's in memory, including information that's supposed to be secure and encrypted. This web comic also explains Heartbleed, should you deem a visualization to be helpful.

Some software engineers believe that the existence of the bug raises questions about the security of C, the code in which the Heartbeat extension was written. Though popular, C is a complex language that offers a lot opportunity for errors in memory management and the handling of values. A bug in another open-source SSL implementation, GnuTLS, cropped up a month before Heartbleed, and was also written in C. That bug was even older; the code responsible for it was added in 2005.

What's the next step?

Human error is ultimately to blame for Heartbleed, but the fault doesn't fall solely on the shoulders of a single coder. OpenSSL is free software used by Fortune 500 companies, governments and even military organizations, yet these outfits almost never contribute funding or manpower to the project.

Companies and governments seem very concerned, yet pledges of real support are ominously absent.

That's a systemic failure on a staggering scale, yet the obvious need for more oversight hasn't spurred many people in positions of great wealth or power to action. OpenSSL Software Foundation money-man Steve Marquess says that donations have increased since the bug's discovery, but, as of April 12, still totaled no more than \$9,000 for the year. Most of that came from individuals pledging \$5 or \$10. Companies and governments seem very concerned, yet pledges of real support are ominously absent.

The world also must learn from this mistake. Using an open-source project without contributing to it is, in the long term, a recipe for disaster particularly when the project is a critical part of network infrastructure. The Internet's security shouldn't be upheld by a handful of volunteers who find their names in the news only when something goes wrong.

## Heartbleed Fixes May Be Slowing Web Browsers

The heartache from the Heartbleed Internet flaw is not over, and some experts say the fix may lead to online disruption and confusion.

The good news is that most sites deemed vulnerable have patched their systems or are in the process of doing so.

The bad news is that web browsers may be overloaded by the overhaul of security certificates, leading to error messages and impacting web performance, said Johannes Ullrich of the SANS Internet Storm Center.

A good percentage of the websites are patched, Ullrich told AFP.

The patches enable the web operators to obtain new security certificates that demonstrate that they can be trusted by web browsers.

But Ullrich noted that for each patch, web browsers must update their list of untrusted certificates or keys that would be rejected.

For the fix, the website needs to obtain a new private key and the old key has to be revoked, he said. Browsers will not trust the old keys.

Browsers usually update dozens of keys on a daily basis, but because of Heartbleed, that may rise to tens of thousands.

If the verification process takes too long, Ullrich said, the browser may simply declare the site invalid or show an error message.

People will see errors, he said. They will see an invalid certificate. They can either accept the certificate or consider it invalid.

The big danger is that people may become so confused or frustrated that they ignore the warnings or reconfigure their browsers to no longer perform the security check.

If people turn off those lists, then a hacker could get in, Ullrich said.

With thousands of websites seeking new security credentials, some certificate authorities and website administrators have been making careless mistakes, online security firm Netcraft noted.

Warnings about the danger have grown over the past week, with everyone from website operators and bank officials to Internet surfers and workers who telecommute being told their data could be in danger.

The bug is a flaw in the OpenSSL encryption at https websites that Internet users have been taught to trust.

The Heartbleed flaw lets hackers snatch packets of data from working memory in computers, creating the potential for them to steal passwords, encryption keys, or other valuable information.

The security firm CloudFlare reported last week that it appeared impossible to use Heartbleed to steal certificates to impersonate a website, but then reversed itself after a challenge to the security community brought out evidence that these thefts were possible.

Google said that some versions of its Android mobile operating system may be vulnerable to Heartbleed. On Monday, it urged developers to create new security keys to ensure that apps and other services can be trusted.

Trend Micro security specialist Veo Zhang said the latest evidence shows mobile phones are potentially vulnerable in two ways.

This is because mobile apps may connect to servers affected by the bug, Zhang said in a blog. However, it appears that mobile apps themselves could be vulnerable. We have found 273 in Google Play which are bundled with the standalone affected OpenSSL library, which means those apps can be compromised in any device.

Some of the first evidence of hackers using Heartbleed has begun to surface in recent days.

British parenting website Mumsnet announced Monday that members data had been accessed, potentially compromising 1.5 million accounts.

Officials in Ottawa said personal data for as many as 900 Canadian

taxpayers was stolen after being made vulnerable by the Heartbleed bug.

The Canadian Revenue Agency last week shuttered its website over concerns about Heartbleed.

### Facebook Home Reception Slower Than Expected

Facebook has been a wildly successful social network, but that doesn't mean it hasn't seen some failures along the way. According to CEO Mark Zuckerberg, Facebook Home was at the top of that list.

In a recent interview with Zuckerberg, the The New York Times made a point that Facebook's homemade features like Facebook Home and Graph Search have been flops. However, the companies it has acquired like Instagram and WhatsApp have been more successful which calls into question Facebook's ability to innovate.

Zuckerberg defended Graph Search, saying that it's more of a long-term investment than Facebook Home. Graph Search is a semantic search engine that was designed to give answers to a user's natural language queries rather than a list of links.

"With Graph Search, I think that modern search products have so much built into them that we knew it was going to be a five-year investment before we got anything really good and different," said Zuckerberg. "So far we've done these milestones. The first one was that we were able to search over structured connections on Facebook. That was important as a consumer product and also as infrastructure that we are using inside the company.

"The next focus is searching posts. All of this has been on desktop, and the real push is mobile. So I'm not that worried about it. I think the real question will be how effective it will be on mobile once post-search works. I think that's a five-year thing. We have to think about it over a longer period of time."

But Zuckerberg was quicker to admit that Facebook Home isn't too popular. Facebook Home is a user interface layer for Android-compatible smartphones, offering notifications and other Facebook-flavored features right on the lock screen.

"With Home, the reception was much slower than we expected," said Zuckerberg. "But it was a riskier thing. It's very different from other apps, let's say Paper or Messenger. For those, you install it, and if it's useful you'll go back to it and use it. Home is your lock screen. When you install it, it's really active, and if it does anything that you don't like, then you'll uninstall it."

Another innovation question brought forth by NYT is why Facebook couldn't develop something like WhatsApp instead of paying \$19 billion USD for the acquisition, since it already had something similar (Facebook Messenger). Zuckerberg said that its Facebook Messenger is quite different from WhatsApp, and are both big in their separate markets.

"I think you want to look at the things that we do in three stages. First, there's Facebook the app. A billion people or more are using it, and it is a business," said Zuckerberg. "Next there's Instagram, WhatsApp, Messenger, Search these are use cases that people use a lot, and they

will probably be the next things that will become businesses at Facebook. But you want to fast-forward three years before that will actually be a meaningful thing.

"Then there are things that are nascent, that we're inventing from scratch, like Home, Paper or any of the other Creative Labs work we're going to do. Maybe in three to five years those will be in the stage where Instagram and Messenger are now. So what we want to do is build a pipeline of experiences for people to have. It would be a mistake to compare any of them in different life cycles to other ones.

"They're in different levels."

### Google Trends Adds Email Notifications

Google has updated its search statistics service, Google Trends, to allow people to sign up to be notified by email periodically about the popularity of specified search terms. Introduced in 2006, Google Trends has long been a popular way to assess what people are looking for online. But the service has been hampered by lack of an API, promised back in 2007, but never delivered. A Google Trends API would allow programmatic monitoring of search trends by software, a more convenient option than requiring people to visit the Google Trends website for manual keyword entry.

In 2008, Google introduced a variation on Google Trends called Google Insights for Search that is tailored to helping advertisers understand search behavior. It doesn't have an API, either. Since then, numerous unofficial Google Trends APIs have been developed.

Asked whether Google still plans to provide a Trends API, a Google spokesperson said, "We don't have any new news to report right now about that."

In a blog post, Google engineer Gavri Smith acknowledges the burden of having to seek information manually on Google Trends. "[W]ithout doing your own exploration on the Trends website, it can be tough to find the interesting - and sometimes surprising - topics the world is searching for," said Smith. "Starting today, it's easier to get just the right insights at just the right time with email notifications."

Consider email notifications a consolation prize of sorts. An API would be a sign that Google wants Trends to become a serious data-mining service. Email notifications indicate that Google sees Trends as a way to enhance consumer engagement.

Trends allows users to subscribe to search topics, country-specific Hot Searches, or any US monthly Top Chart. It's similar to Google Alerts, except that Alerts provides links to newly indexed content associated with specified search terms. Trends provides graphs describing the frequency of specified search terms, or what's popular in broad categorical topics over time.

As such, Trends has limited utility beyond satisfying personal curiosity. You could use it, for example, to receive a weekly email update on the popularity of a term such as "Bitcoin." But the inability to drill down into the details of the data, to segment and process them, makes the



service more of a social yardstick than a tool for serious data science.

One option that would help make Trends more useful is a way to trigger notifications based on search surges. Currently, Trends will send out notifications on a weekly or monthly basis, subject to an unspecified degree of variation. Greater real-time awareness and responsiveness would make the service more useful for urgent matters. For example, a human rights organization might find it valuable to be notified immediately if searches for the name of an at-risk individual suddenly increase. But it remains to be seen whether Google wants to turn Trends into something more than a casual research tool.

### The Newest Facebook Feature: Sharing Your Location with Friends

Facebook knows a lot about you, including, in many cases, the location you're posting from. Now the social network wants other people to know where you are, too.

On Thursday, Facebook announced that it will be rolling out a new feature called Nearby Friends. The feature will allow you to see your approximate distance from anyone within your network. You'll also be able to continuously share your location with other people for a limited amount of time.

The good news? It's an opt-in feature, meaning it'll be enabled only for those who want to use it.

It works like this: Once the feature becomes available to you on iOS or Android in the next couple of weeks, you'll see the Nearby Friends option in the app list on your navigation menu. You can choose to turn it on for your entire social network, or to limit the people who can see your location to a specific friend list.

Then a list of your (geographically) closest friends will show up, ranked by how many miles they are from you. Again, you'll see only the people who have also turned on the feature and allowed you to see them. The list will display a timestamp next to each person so that you'll know exactly when Facebook registered her location. Finally, if you're in a metropolitan area, the app will do you the favor of including the name of the neighborhood the person is in.

A location-services feature like this is not at all novel. Foursquare's entire business revolves around whether you can see if your friends have checked in around you. And the now-defunct Google Latitude worked with the company's Maps app to do essentially the same thing as Nearby Friends. There are even entire apps, like Connect, SocialRadar, and Cloak, that are dedicated to culling the information provided by your friends' social networks in order to map the location of their last digital interaction (so you can either connect with them or avoid them).

What's somewhat eerie about this feature, however, is how expansive each Facebook member's social network remains. Facebook is a community where family, friends, colleagues, and old high-school acquaintances congeal into one large blob of connections unless you are constantly pruning your sharing settings. If you forget to leave your Nearby Friends feature off, it could potentially allow for less-than-comfortable stalking from your friends and family.

For now, it seems that Facebook has made it easy to differentiate who you're sharing your current location with. But as even Facebook CEO Mark Zuckerberg's sister has proved, it hasn't always had the best reputation for making matters of privacy easy to understand.

If you do choose to try it out, I'd recommend making a list of trusted friends you feel comfortable sharing your location with. That way you never risk airing your private information to an audience of strangers.

### Google's Recent TOS Update Reminds Us What Little Choice We Have

So, Google analyzes your email. Who knew? Well, judging by a recent wave of internet chatter regarding a two-sentence update the search giant made to its terms of service this week, not that many. The truth is, of course, that most Gmail users did know that Google scans your email, or parses it in some way so that it can place those oh so important personalized adverts alongside them. Like anyone on Facebook who got dating ads after changing their relationship status can attest to. The backlash this week, however, seemed to take two basic flavors. One being paranoia that some deep change had taken place that the search giant was looking to sneak past us. The second being that this was a sign of how our rights are constantly being eroded, and that this constant "policy creep" will soon have us handing over our deepest darkest digital secrets, without any powers to negotiate. So which is it?

We asked Google directly, and it tells us that on this occasion, the additional text is merely a clarification of the existing policy. It's spelling out what it already does. We spoke to London-based media lawyer John Haggis about this kind of amendment, who confirmed that if there were significant changes to the meaning of the policy, then Google (and others, like PayPal's shown below) would have an obligation to communicate that to its users. Not doing so would be an incredibly risky strategy for any firm. Minor housekeeping and clarifications, however, might not warrant a (potentially alarming) email blast -- though this recent Google case shows that it's still worth considering your strategy every time.

For those that were concerned about the specific part in Google's TOS that refers to email you receive (i.e., that sent by people who might not have agreed to said TOS), Haggis reminds us to think along the lines of how images, etc. are shared on Facebook. You might not be on Mark Zuckerberg's social network, but a photo you took and sent to a friend could be. Facebook might even learn it's a picture of you via tagging, and have a moderate profile of you based on multiple such photos. But, the truth is, there's not a lot it can do with that information if you're not a signed-up (and contractually agreed) member.

The more important issue highlighted by Google's recent tweak is of what little choice we have either way. It serves as another reminder that some of our most precious data is locked into services and ecosystems that we can do little to control or negotiate with. If your email provider incrementally changes its terms of service, you might not even really know what you've agreed to anymore. Worse, you could actually know all too well, and decide that you no longer are comfortable with those conditions. But what are your options, then, if a service goes a bullet-point too far? For the most part, you're left with the binary choice of suck it up, or find another provider. Here lies the biggest

problem facing you or me. Who wants to change their email address after double figure years of distribution? Or migrate their music collection from one corner of the cloud to another (not to mention whether you can take it with you thanks to rights restrictions). Not many we'd wager.

The good news? Google tells us that for future such amendments it will be placing an "Updated" notice on the Google.com homepage (including on mobile), which will also show on regional domains (Google.co.uk, for example) when applicable. This might not solve your data-hostage quandary, but it should mean fewer false alerts.

#### Laptop Used for First U.S. Presidential Email Sells for Over \$60,000

The laptop computer that Bill Clinton used in 1998 to send the first-ever U.S. presidential email has sold for \$60,667 in an online auction, the Boston auction house that handled the transaction said Thursday.

RR Auction did not disclose the name of the buyer of the still-functional Toshiba Satellite that Clinton borrowed to email veteran astronaut John Glenn, who was orbiting Earth aboard the space shuttle Discovery.

The laptop, with accessories and full documentation, originally belonged to White House physician Robert Darling, who lent it to Clinton when NASA informed the president that Glenn wanted to swap emails with him.

It s a remarkable collection that represents the dawn of a new age, combining America s greatest technological achievements space travel and the Internet, said RR Auction vice president Bobby Livingston in a statement.

Glenn, a U.S. senator who in 1962 became the first American astronaut to orbit the Earth, was completing a nine-day mission on Discovery in November 1998 when he sent word that he wanted to email Clinton, who at the time was visiting friends in his home state of Arkansas.

This is certainly a first for me, writing to a president from space, and it may be a first for you in receiving an email direct from an orbiting spacecraft, wrote Glenn, then 77.

Clinton was keen to get the message, but when his staff couldn t readily find him a computer to do so, Darling stepped forward with his trusty Toshiba and his personal AOL email address.

Hillary and I had a great time at the launch, emailed Clinton, referring to Discovery s liftoff from the Kennedy Space Center a few days earlier.

We are very proud of you and the entire crew, and a little jealous.

In an interview in 2000, Clinton said he never used email due to security concerns, but acknowledged emailing Glenn in space, as well as some U.S. marines and sailors at sea at Christmas.

Prior to selling the laptop in 2000, Darling took care to keep the historic email exchange on its hard drive, and made a copy on its internal floppy drive, while deleting all other data.

He also typed up a memo about the landmark email, saying Clinton seemed

to really enjoy himself particularly when he pressed the send key and realized that at that instant his message was traveling through cyberspace and into real space.

## Google Glass Sells Out, But More Chances To Buy May Come Soon

Google's one-day sale of Glass was a success at least, according to Google.

On Tuesday, the company held a one-day sale where anyone U.S.-based adult could buy the \$1,500 prototype headset (while supplies lasted), and become a member of the company's Glass Explorers program. On Wednesday, Google said it had sold every available Glass it had set aside for the day-long promotion. Still, Google isn't saying just how many pairs it sold.

The company did, however, tease at the fact that it may open Glass up for sale again before the wearable tech becomes a consumer product. (Google's now saying sometime before the end of the year, but we've heard that before.)

If you missed it this time, don't worry, the company said on its Google+ page for Glass. We'll be trying new ways to expand the Explorer program in the future. There's a form you can fill out at [glass.google.com](http://glass.google.com) if you are interested in the next chance to pay up to become one of Google's beta testers.

## Google Offering Try-before-you-buy Kits to Those Interested in Glass

Google has begun contacting customers and offering them the chance to try out the company's Glass wearable device before committing to pay \$1,500 for the gadget.

The company is offering to send those users trial kits that come with Glass units in four different color options along with the device's various frame styles.

"We've heard from potential Explorers that they'd love to be able to try Glass on at home before committing to purchase it," a Google spokeswoman said in a statement. "As a result, we're doing outreach to a small group to see how this approach works. We'll let you know if this experiment continues."

Before sending out the kits, Google places a \$50 hold on customers' credit cards so that users will not be tempted to keep the gadgets.

The devices that Google sends out in the kits appear to be Glass units that have been returned by other customers. However, the kit's Glass devices have had their USB ports "destroyed" so that their batteries cannot be recharged, rendering them inoperable, according to 9to5Google.

Recently, Google also held a one-day sale for Glass where any adult U.S. resident could purchase the \$1,500 device without needing an invitation to do so.

Google has said that it will begin selling the device to the general

public at some point in 2014, but right now, the company appears to be trying to get early editions of the gadget to as many users as possible.

### Google Has Developed Technology To Crack CAPTCHAs

Google has cracked the CAPTCHA. In a paper published this week, Google researchers say that they've developed an algorithm that can accurately solve Google's own CAPTCHA puzzles — those obfuscated jumbles of letters and numbers you type in on websites to prove that you're human — with 99.8 percent accuracy, obviously posing something of a problem to the puzzle's intended purpose of weeding out robots. The new system was developed to help Google automatically analyze hard-to-read signs and house numbers photographed by its Street View cameras, allowing it to accurately match images with locations on a map.

Despite being near perfect when it comes to CAPTCHAs — a feat that plenty of humans can't even manage — the new system's analysis of Street View imagery isn't quite as accurate, correctly identifying the text just over 90 percent of the time. When analyzing house numbers specifically, however, its accuracy jumps up to over 96 percent.

Google is, of course, specially suited to developing such advanced automated text analysis because of its extensive work with Street View and reCAPTCHA, its own CAPTCHA service. Even so, Google says that it's already found ways to further protect reCAPTCHA from being broken by others' computers. Thanks to this research, we know that relying on distorted text alone isn't enough, Vinay Shet, reCAPTCHA's product manager writes in a blog post. Shet explains that part of this is analyzing a user's full interaction with the CAPTCHA puzzle — and not solely whether they can get the answer right.

~~~~~

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.